ahia
Assoc. of Healthcare Internal Auditors

NEW PERSPECTIVES

on Healthcare Risk Management, Control and Governance

www.AHIA.org Journal of the Association of Healthcare Internal Auditors Vol. 39, Number 2, Summer 2020

Sell Your Audit Ideas

Adopt six proven actions

page 7

Fight Identity Fraud

Audit Use of the Limited Access Death Master File

page 14

Hire a Construction Audit Consultant

Actively participate for best results

page 20

The Opioid Crisis

Address the risks of prescribing and misuse

page 26

Business Email Compromise

Avoid becoming a victim

By Victor Hartman, JD, CPA, CFF, CFE

By now, most of us have heard of the business email compromise (BEC). The fraud has produced nearly 70,000 victims with losses totaling in excess of $10 billion reported to the Federal Bureau of Investigation's Internet Crime Center (IC3) during the period October 2013 through July 2019.[1] The actual numbers likely far exceed these losses, as many victims will not report their losses to law enforcement.

The scam involves convincing an organization insider to wire transfer funds to the fraudster. At first glance, this scam seems implausible. Certainly, organizations have internal controls that would prevent this fraud. Yet the ever-growing number of victims worldwide tells us otherwise. You must educate employees with financial responsibilities about the various techniques fraudsters will employ.

In September 2019, the U.S. Department of Justice announced in a press statement the arrest of 281 individuals in a worldwide enforcement action involving the BEC. The action was a coordinated effort involving law enforcement in nine countries.[2]

As funds in a BEC scam typically move through several countries before landing in the fraudsters' country, successful investigation and apprehension of these individuals takes an international effort. Despite these efforts by law enforcement, you must be vigilant in helping your organization avoid becoming a victim to these and related frauds.

BEC steps

- Victim is identified
- Victim is groomed
- Victim accepts wiring instructions
- Victim transfers funds

Victim is identified

Identifying a victim is the first of the four basic steps of BEC. Organized groups of fraudsters will target an organization, most often U.S. and European organizations. Although the fraudsters are often from Nigeria or Eastern European countries, they could be from anywhere.

The victims can be any type of organization as well. Organizations that deal in international purchases are common victims as well as those that deal with the purchase and sale of real estate.

[1] www.ic3.gov/media/2019/190910.aspx
[2] www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds

The easiest schemes for fraudsters are victims simply responding to a social engineering attack.

Victim is groomed

The fraudsters are primarily looking for low hanging fruit. After they have identified a target, grooming begins. The grooming step can include spear phishing, social engineering, email spoofing, and the use of malware. Although the techniques vary, the fraudsters want to find a way to communicate with a financial insider via email.

The easiest schemes for the fraudsters are the ones where a victim simply responds to a social engineering attack. For example, the fraudster may communicate with the victim organization pretending to be one of their vendors. Using a pretext communication, the apparent vendor emails or telephones the accounts payable clerk with a request to change the bank routing and account numbers.

A more complicated method is where the fraudsters take over the administrator rights of the organization's email system. The takeover can be done through a social engineering scheme where an unsuspecting employee downloads malware. The organization's inadequate defenses allow the malware to compromise the email system.

Once the fraudster and victim are communicating, the fraudster may ask questions or give instructions like:

- Can we make a transfer today?
- What is your daily limit on international transfers?
- We need to make a payment to a vendor.
- Please assist me in updating the direct deposit of my salary.

Take the case where the fraudsters have penetrated the victim organization's email system. An email that appears to come from the CEO instructing someone in finance to urgently pay a vendor can be highly effective. Regardless of the scenario, after some email exchanges, the financial insider is convinced he or she is dealing with a legitimate party.

Victim accepts wiring instructions

The victim now accepts the wiring instructions from the fraudster. Depending on the ruse, this step may involve a one-time wire transfer to the victim. Alternatively, if the fraudster has the victim successfully change the bank routing and account numbers of a vendor, the fraudster can keep accepting payments from the victim.

The fraud continues until the real vendor contacts the victim organization and complains of not receiving funds owed. The victim organization may have sent hundreds of thousands of dollars to the fraudsters before the scheme is caught.

Victim transfers funds

The victim transfers funds to a bank account controlled by the fraudsters. The funds are likely to go to a Hong Kong or other Chinese bank and then sent to the fraudsters' country of origin.

A preventive tip to a potential victim can be provided by the routing number of the transfer. Unless the victim organization was intending to send the funds to China, the routing number will provide a clue on the funds' first stop.

Bank routing numbers are easily found on the internet and can be compared against the vendor's intended bank's location. If the funds are directed to a Chinese bank, but the funds should go to a vendor in the Philippines, a quick look up and comparison of the bank routing number can stop a fraudulent transfer in its tracks.

The whole process may take a few days or several weeks. However, for the persevering fraudster, the rewards can be great.

Protection controls

What can be done to protect your organization? Exhibit 1 summarizes the FBI's list of prevention controls.

Unfortunately, even when vigorously following these guidelines, an organization may still fall victim to a BEC. Once an organization has learned they have been victimized in a BEC scam, time is of the essence. The victim has 24 to 72 hours to contact both the bank and the FBI.

Persistence should be used in getting through to the correct FBI official. The FBI has protocols with various banks to stop the funds. Stopping the funds will only be effective if the victim quickly realizes the fraud and promptly notifies authorities.

An email that appears to come from the CEO instructing someone in finance to urgently pay a vendor can be highly effective.

Exhibit 1- Prevention controls

1. Monitor all financial accounts.
2. Keep all software and systems up to date.
3. Create intrusion detection system rules that flag emails with extensions that are like your organization's email. For example, legitimate email of abc_company.com would flag fraudulent email of abc-company.com.
4. Create an email rule to flag email communications where the reply email address is different from the from email address shown.
5. Color code virtual correspondence so that e-mails from employee/internal accounts are one color and emails from non-employee/external accounts are another.
6. Verify changes in vendor payment location by adding additional two-factor authentication such as having secondary sign-off by organization personnel.
7. Confirm requests for transfers of funds by using phone verification as part of a two-factor authentication. Use previously known numbers, not the numbers provided in the email request.
8. Scrutinize all email requests for transfer of funds to determine if the requests are out of the ordinary.

Source: www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

Related fraud

The BEC scams are often related to, and conducted with, other forms of fraud.

Romance scams – The victims are lulled into believing they are in a legitimate relationship. The victims are tricked into sending or laundering money under the guise of assisting the paramour with an international business transaction, a U.S. visit, or some other cover story.

Employment opportunities scams – The victims are convinced to provide their personally identifiable information to apply for work-from-home jobs. Once the victims are hired and overpaid by a bad check, they are convinced to wire the overpayment to the employer's bank before the check bounces.

Fraudulent online vehicle sales scams – The victims are convinced to purchase a nonexistent vehicle and must pay by sending the codes of prepaid gift cards in the amount of the agreed upon sale price to the seller.

Rental and lottery scams – The scammer agrees to rent a property, sends a bad check in excess of the agreed upon deposit, and requests the overpayment be returned via wire before the check bounces. Lottery scams involve victims who are convinced they won an international lottery but must pay fees or taxes before receiving the payout.

Conclusion

The BEC fraud is not going away anytime soon because the scam is too profitable for the fraudsters who have little chance of getting caught. Most importantly, organizations should adopt the attitude that they could become a victim.

Make sure your organization can defend against BEC. All employees with responsibility for establishing vendor accounts or with accounts payable functions, and those with ACH or wiring authority, must be periodically trained on this fraud. Further, management must create an atmosphere where any employee that suspects the BEC is at play feels comfortable with challenging management about a payment instruction. Organizations of all types must be vigilant in educating their employees and implementing procedures to deter this fraud. **NP**

Victor Hartman, JD, CPA, CFF, CFE, is Principal of The Hartman Firm, LLC, specializing in forensic accounting and internal investigations. He was an FBI Special Agent. He is now an Adjunct Professor at Georgia State University and serves on Georgia Southern University's Forensic Accounting Advisory Board. Vic can be reached at (404) 369-0616 and Vic@Hartmanfirm.com.